P591

Prescription sur la cyberprotection et la sécurité des données. Instructions pour les systèmes rattachés à la plateforme NOVA et leurs utilisateurs.

Édition du 11 décembre 2023

Modifications valables à partir du 1er janvier 2024

Chapitre/chiffre	Modifications

Alliance SwissPass Länggassstrasse 7 3012 Berne Tel +41 31 359 22 40
info@allianceswisspass.ch allianceswisspass.ch

Table des matières

0 Remarques préliminaires 3
0.1 Généralités et but 3
0.2 Glossaire 3
1 Champ d'application 5
1.1 Représentation graphique 5
1.2 Contact 5
2 Exploitants et utilisateurs concernés 6
2.1 Utilisateurs de la plateforme NOVA 6
2.2 Exploitant NOVA 7
2.3 Processus d'accès à la plateforme NOVA 7
3 Autres dispositions 8
3.1 Désactivation pour des raisons de sécurité 8
3.2 Droit d'audit 8
3.3 Mesures techniques et organisationnelles 8
3.4 Responsabilité et garantie 8
3.5 Exclusion d'un utilisateur 9
3.6 Entrée en vigueur et délai transitoire 9

0 Remarques préliminaires

0.1 Généralités et but

La présente prescription fixe des standards contraignants en faveur de la sécurité de l'information pour les utilisateurs de la plateforme NOVA. Les recommandations existantes en matière de cybersécurité, comme le standard minimal pour les TIC, le «Manuel sur la cybersécurité destiné aux entreprises de transports publics» ou les normes pertinentes telles l'ISO 27001 ou le cadre NIST, ont été utilisées comme références lors de l'élaboration de la présente P591.

L'accent est mis sur la réalisation technique de mesures tirées de ces références selon un principe de «défense en profondeur» de la sécurité de l'information.

Toutes les modifications de fond de la présente prescription (compléments, modifications, suppressions, etc.) relèvent de la compétence de la commission Distribution (KoV) de l'Alliance SwissPass, conformément au règlement des compétences, chiffre 7 du règlement d'organisation de la C500. L'organe de gestion de l'Alliance SwissPass est chargé de faire respecter ces règles.

Outre la présente Prescription 591, les réglementations suivantes valent en particulier en matière de cyberprotection et de sécurité des données (liste non exhaustive):

- Conditions d'utilisation de NOVA (C500, annexe 12)
- Réglementation sur l'utilisation des données dans les TP (C500, annexe 16)

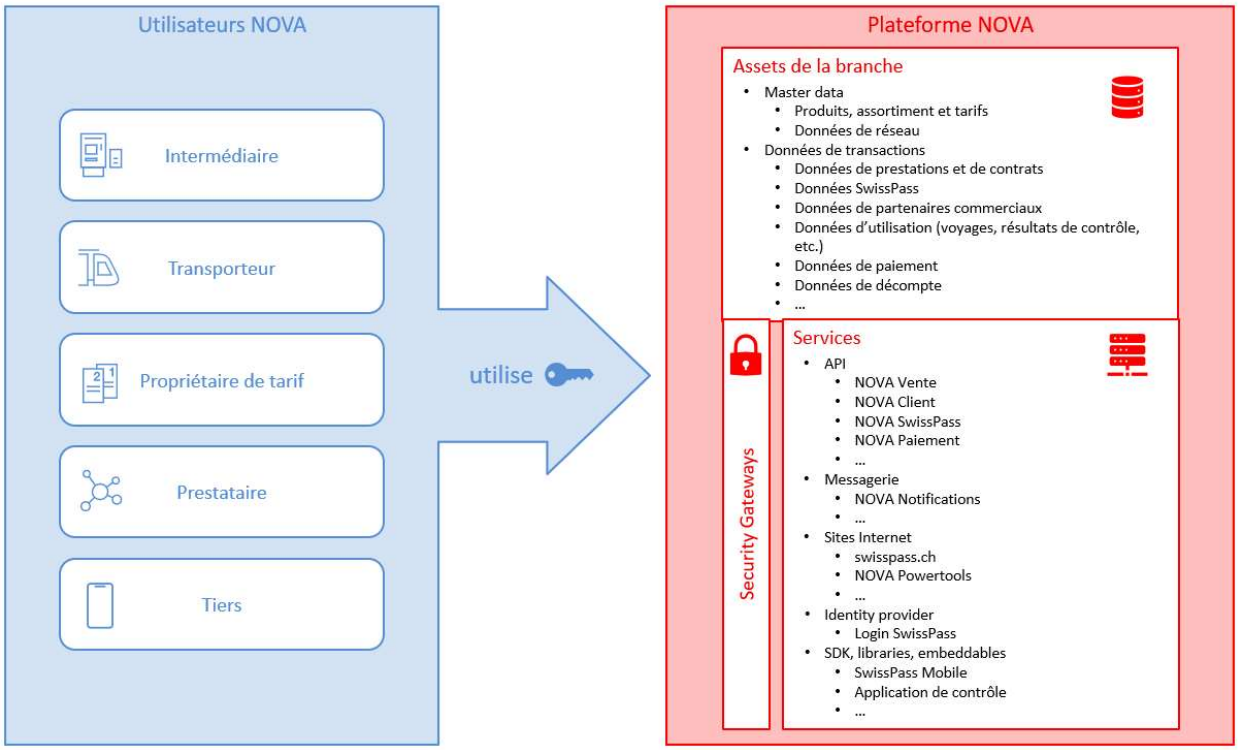
0.2 Glossaire

Alliance SwissPass	Organisation de la branche des transports publics, regroupant 250 entreprises de transport et 18 communautés, s'engageant au niveau suisse pour des dispositions tarifaires harmonisées, compréhensibles et économiques, des solutions de distribution modernes et attrayantes et des assortiments et systèmes d'information axés sur la clientèle.
analyse des causes racines	Processus déterminant les causes profondes de problèmes afin de trouver des solutions appropriées. En anglais *root cause analysis* (RCA).
C500, Convention 500	Contrat de collaboration de la branche réglant les compétences au sein de l'Alliance SwissPass.
CFF	Chemins de fer fédéraux suisses SA
CISO	Abréviation de «*chief information security officer*», responsable de la sécurité des systèmes d'information en français.
communauté	Communauté d'abonnement, de tarif ou de trafic selon les tarifs 651.xx
CVSS	Abréviation de «*Common Vulnerability Scoring System*», soit un standard industriel pour évaluer le niveau de gravité de lacunes possibles ou effectives de sécurité dans des systèmes informatiques (utilisé ici dans la version 3).
cyberprotection	Ensemble de mesures visant à protéger et défendre des ordinateurs, des serveurs, des appareils mobiles, des systèmes électroniques, des réseaux et des données contre toute attaque malveillante du cyberespace.
DE-OCF	Dispositions d'exécution de l'ordonnance sur les chemins de fer

ETC	entreprise(s) de transport concessionnaire(s)
exploitant NOVA	Mandataire chargé par l'Alliance SwissPass de l'exploitation des systèmes et infrastructures de NOVA → plateforme NOVA
intermédiaire(s)	Organisation(s) vendant des assortiments NOVA en représentation d'une ou de plusieurs entreprises de transport prestataires. Le terme comprend les entreprises de transport au titre d'une concession de l'OFT, les gestionnaires d'une infrastructure ferroviaire, les communautés tarifaires et de trafic et les tiers rattachés à NOVA.
ISMS	Abréviation d'«*Information Security Management System*», soit un système de gestion de la sécurité de l'information. Il s'agit du recueil de procédures et de règles d'une organisation servant durablement et constamment à définir, guider, contrôler, maintenir et améliorer la sécurité de l'information.
ISO 27001	La norme ISO 27001 est une norme internationale sur la sécurité de l'information.
KoV	commission Distribution de l'Alliance SwissPass
NIST	Le «Cybersecurity-Framework» du *National Institute of Standards and Technology* étasunien comporte des instructions détaillées et des bonnes pratiques permettant aux entreprises les respectant d'améliorer la gestion des risques relatifs à la sécurité de l'information et à la cybersécurité.
OFT	Office fédéral des transports
organe de gestion de l'Alliance SwissPass	Organe gérant les affaires de l'Alliance SwissPass selon la Convention 500.
plateforme NOVA	Plateforme nationale de distribution des titres de transport des transports publics suisses. De l'allemand «*Netzweite ÖV-Anbindung*».
prestataire	Personne physique (être humain habilité en droit) ou morale (entreprise, organisation, etc.) fournissant une prestation.
propriétaire de tarif	Instance exerçant la souveraineté tarifaire (Service direct national, service direct régional [communauté tarifaire ou de trafic], entreprise de transport).
standard minimal pour les TIC	«Norme minimale pour améliorer la résilience informatique» de l'Office fédéral de l'approvisionnement économique du pays (OFAE)
tiers	Organisation rattachée à la plateforme NOVA et servant d'intermédiaire pour l'assortiment NOVA, n'étant ni une entreprise de transport au titre d'une concession de l'OFT, ni un gestionnaire d'infrastructure ferroviaire, ni une communauté tarifaire ou de trafic suisse.
TP	transports publics
transporteur(s)	Prestataire(s) réalisant des transports physiques (p. ex. une entreprise de transports publics ou un taxi) ou exploitant une infrastructure ou un véhicule qu'il possède (p. ex. Mobility). S'y ajoutent toujours plus d'«intermédiaires» proposant non pas directement de services de mobilité, mais des offres correspondantes en les combinant parfois (p. ex. Whim, moovel).
utilisateurs NOVA	L'ensemble des utilisateurs de la plateforme NOVA, soit les intermédiaires, les transporteurs, les propriétaires de tarif et les prestataires.
vente	On entend par «vente» l'ensemble du processus de vente de titres de transport des transports publics, commençant par l'information et le conseil au voyageur, suivi par la vente en tant que telle et le paiement, et incluant encore le contrôle et le service après-vente (échange, annulation, remboursement, réclamation).

1 Champ d'application

1.1 Représentation graphique



La présente prescription met l'accent sur les acteurs indiqués en bleu ci-dessus, soit les utilisateurs de NOVA, qui échangent des données entre la plateforme NOVA et leurs propres systèmes d'informations (canaux de distribution, points de vente, appareils de contrôle, etc.).

Autres définitions: les **intermédiaires** vendent des assortiments NOVA en représentation d'une ou de plusieurs entreprises de transport prestataires. Les **transporteurs** effectuent les transports physiques. Les **propriétaires de tarif** sont les instances qui possèdent la souveraineté sur les tarifs concernés. Les **prestataires** fournissent une prestation. Les **tiers** sont des organisations rattachées à la plateforme NOVA qui font office d'intermédiaires dans la vente de l'assortiment NOVA. Les utilisateurs NOVA peuvent jouer plusieurs rôles.

1.2 Contact

En cas de questions sur la présente prescription, merci de vous adresser à:

Alliance SwissPass
c/o ch-integral
Länggassstrasse 7
3012 Berne

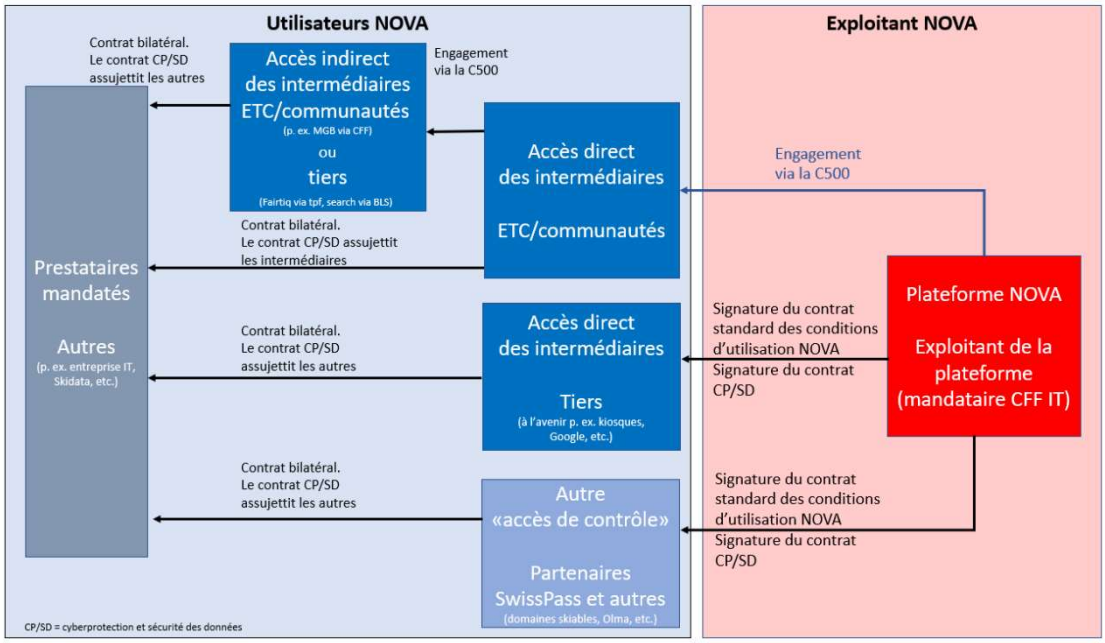
tarife@allianceswisspass.ch

2 Exploitants et utilisateurs concernés

Tous ceux qui recourent à la plateforme NOVA sont dénommés ci-après «utilisateurs NOVA», qu'ils participent directement ou indirectement à la plateforme ou qu'ils soient chargés de fournir une prestation.

2.1 Utilisateurs de la plateforme NOVA

Les possibilités suivantes sont données quant à l'utilisation de la plateforme NOVA:



Accès direct des intermédiaires: les intermédiaires soumis à la C500 peuvent directement se rattacher à la plateforme NOVA. La réglementation correspondante s'applique.

Accès direct des tiers: les tiers qui souhaitent vendre des prestations de TP peuvent directement se rattacher à la plateforme NOVA, à condition qu'ils aient signé le contrat standard des conditions d'utilisation de NOVA et celui relatif à la cyberprotection et à la sécurité des données. Ce dernier assujettit les tiers à la présente P591.

Accès direct des partenaires SwissPass et autres: les partenaires SwissPass et les autres utilisateurs employant le SwissPass pour fournir leur prestation (p. ex. en tant que transporteurs) peuvent identifier leurs clients via le SwissPass ou utiliser un accès de contrôle, à condition qu'ils aient signé le contrat standard des conditions d'utilisation de NOVA et celui relatif à la cyberprotection et à la sécurité des données. Ce dernier assujettit les partenaires SwissPass et autres à la présente P591. L'exploitant NOVA reçoit un double de cette convention.

Accès indirect des intermédiaires: d'autres intermédiaires soumis à la C500 (comme les ETC et les communautés) et les tiers souhaitant vendre des prestations de TP peuvent se rattacher à la plateforme NOVA de manière indirecte, c'est-à-dire via l'accès d'un intermédiaire soumis à la C500 et directement rattaché. Les participants indirects ne sont pas autorisés à octroyer l'accès à la plateforme (la vente des prestations TP) à d'autres personnes ou entreprises (pas de sous-accès). Les utilisateurs soumis à la C500 doivent

la respecter. Les tiers doivent avoir signé le contrat standard des conditions d'utilisation de NOVA et celui relatif à la cyberprotection et à la sécurité des données. Ce dernier assujettit les intermédiaires indirects à la présente P591.

Prestataires mandatés: l'implication de prestataires est possible en tout temps. L'exploitant NOVA doit être informé avant toute collaboration. Les prestataires impliqués sont des auxiliaires au sens de l'art. 101 CO. L'art. 399, al. 2 CO est expressément exclu. Les utilisateurs NOVA doivent signer une convention avec le prestataire impliqué et y lier les obligations tirées de la présente P591. L'exploitant NOVA reçoit un double de cette convention. Le contrat relatif à la cyberprotection et à la sécurité des données assujettit les prestataires mandatés à la présente P591. Si les prestataires mandatés impliquent d'autres sous-prestataires, les mêmes obligations valent pour ceux-ci.

2.2 Exploitant NOVA

L'exploitant NOVA est le mandataire chargé par l'Alliance SwissPass qui obtient la souveraineté sur le contrôle des standards minimaux à respecter quant aux exigences, à la mise en œuvre et à la surveillance des prescriptions techniques relatives à la cyberprotection et à la sécurité des données.

2.3 Processus d'accès à la plateforme NOVA

En signant le contrat d'utilisation de la plateforme NOVA, le partenaire contractuel confirme remplir entièrement la présente P591.

3 Autres dispositions

3.1 Désactivation pour des raisons de sécurité

Lors d'un incident de sécurité, l'exploitant NOVA peut immédiatement désactiver temporairement certains canaux ou utilisateurs NOVA. C'est seulement une fois qu'une preuve de la résolution du problème sur la base d'une analyse de causes racines a été approuvée par l'exploitant que ce dernier réactive le canal ou l'utilisateur suspendu. Les charges relatives à l'incident incombent à l'utilisateur ou aux utilisateurs en cause.

3.2 Droit d'audit

Avant la mise en service et pendant l'utilisation (p. ex. lors d'un nouveau release ou en cas d'incident), l'exploitant NOVA a le droit de vérifier le respect de la présente P591, ou de le faire vérifier par une société indépendante. L'utilisateur concerné doit fournir les accès, habilitations et aides demandés pour la réalisation de l'audit. S'il refuse l'accès aux systèmes et documents selon cette disposition, l'exploitant suspend l'utilisateur concerné.

Si l'auditeur constate des manquements, l'utilisateur peut être contraint de participer aux coûts de l'audit. À partir d'un manquement de niveau 7 du CVSS, l'utilisateur assume l'ensemble des coûts.

3.3 Mesures techniques et organisationnelles

Tous les utilisateurs de NOVA sont tenus de respecter les prescriptions et mesures techniques de l'annexe à la présente P591.

3.4 Responsabilité et garantie

L'Alliance SwissPass et l'exploitant NOVA ne donnent aucune garantie relativement à la disponibilité de la plateforme NOVA. Les utilisateurs prennent acte que la plateforme peut être disponible de manière limitée ou complètement indisponible en raison de travaux de maintenance, de dérangements techniques ou d'autres motifs.
L'Alliance SwissPass et l'exploitant NOVA n'assument aucune responsabilité quant à des dommages indirects ou consécutifs, à un manque à gagner, à des pertes de recettes, à une diminution de la valeur de l'entreprise ou à des économies manquées de la part des utilisateurs NOVA.

Les utilisateurs NOVA prennent acte que les contrats conclus avec leurs clients finaux (consommateurs) sont établis directement entre eux et le transporteur ou le prestataire tiers. L'Alliance SwissPass et l'exploitant NOVA n'assument aucune responsabilité quant à ces contrats. Si l'un d'entre eux est rendu responsable en la matière, les utilisateurs NOVA le libèrent et prennent à leur charge les coûts de la défense juridique.

Les utilisateurs directement rattachés à la plateforme NOVA sont responsables du comportement des utilisateurs rattachés indirectement par leur biais, du comportement des prestataires qu'ils mandatent (p. ex. sous-traitants, tiers) et de leurs propres actions. Ils sont tenus de conclure une convention de données contractuelles avec les prestataires mandatés.

3.5 Exclusion d'un utilisateur

Tout utilisateur NOVA violant la présente P591 se voit imposer, par écrit, un délai approprié par l'exploitant NOVA pour résoudre le problème. Si la violation perdure après le délai écoulé, l'utilisateur reçoit un rappel avec un dernier délai de réparation. Il est averti du fait qu'en cas de non-respect de ce délai, il pourra être exclu de l'utilisation de la plateforme NOVA.

Tout utilisateur NOVA violant la présente P591 à plusieurs reprises peut également être exclu de l'utilisation de la plateforme, après avoir été averti des conséquences en cas de récidive.

L'exploitant NOVA se réserve le droit de désactiver en tout temps un utilisateur NOVA à titre temporaire pour des raisons de sécurité, conformément au chiffre 3.1.

3.6 Entrée en vigueur et délai transitoire

La présente P591 entre en vigueur au 1er janvier 2024 selon la décision de la KoV du 11 décembre 2023. Les utilisateurs NOVA déjà rattachés bénéficient d'un délai transitoire unique de douze mois pendant lequel ils doivent fournir une autodéclaration dans les six premiers mois. Les lacunes constatées et les mesures correspondantes doivent être documentées et réalisées selon un plan de mise en œuvre.